#7/Amdt A
6/20/03
CMoore

I hereby certify that this correspondence is being deposited by FACSIMILE to the Commissioner of Patents and Trademarks, Washington, DC on June 12, 2003 by Colleen Dew.

Colleen J. Dew

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Group Art Unit 2876

In re application of	:	June 12, 2003
Kohji Takano et al.	:	Examiner: Edwyn Labaze
Serial No. : 10/023,147	:	
Filed: December 18, 2001	:	IBM Corporation Dept. 18G/Bldg, 300-482
Title: ARITHMETIC CIRCUIT TO INCREASE THE SPEED FOR A MODULAR MULTIPLICATION FOR A PUBLIC KEY SYSTEM FOR ENCRYPTION	:	2070 Route 52 Hopewell Junction, NY 12533-6531

Amendment

Commissioner for Patents and Trademarks
Washington, D.C. 20231

Sir:

1. (original) An arithmetic circuit comprising:

a plurality of registers;

an arithmetic unit, for regarding, as inputs, values entered in said multiple registers; and

a plurality of memories, wherein reading of multiple variables from said plurality of memories to said plurality of registers is performed during the same reading cycle by way of a pipeline process performed by said arithmetic unit.

A1

2. (original) The arithmetic circuit according to claim 1, wherein said arithmetic unit is a multiplier adder for, based on values x_1, x_2, x_3 and x_4 having an r-bit length that are respectively input to a first register, second register, third register and fourth register, providing a result Q for $x_1 + x_2 \cdot x_3 + x_4$ having a length of 2r bits or 2r+1 bits.

3. (original) The arithmetic circuit according to claim 2, wherein said multiple memories include a first memory and a second memory; and wherein, at a stage for writing an operation result, which follows the operation stage of said pipeline process, lower r bits Q_L of said operation result Q are recorded in said first memory, and upper bits Q_H of said operation result Q, excluding said bits Q_L, are recorded in said fourth register, while at a stage for reading variables from said registers, which follows said writing stage, simultaneously, a variable x_1 is read from said first memory and is stored in said first register, and a variable x_3 is read from said second memory and is stored in said third register.

4. (original) The arithmetic circuit according to claim 3, wherein said first m mory and said second memory are two-port memories having one data writing port and one data reading port.

5. (original) The arithmetic circuit according to claim 3, wherein said first memory is a two-port memory having one data writing port and one data reading port, while said second memory is a single-port memory having one port for the writing and reading of data.

a1

6. (original) The arithmetic circuit according to claim 1, wherein said arithmetic unit is a multiplier adder for, based on values x_1, x_2, x_3, x_4 x_5 and x_6, having an r-bit length, that are respectively input to a first register, a second register, a third register, a fourth register, a fifth register and a sixth register, and for providing the operation results Q for $x_1 + x_2 \cdot x_3 + x_4 \cdot x_5 + x_6$, which have a length of 2r bits or 2r+1 bits.

7. (original) The arithmetic circuit according to claim 6, wherein said multiple memories include a first memory, a second memory and a third memory; wherein, at a stage for writing an operation result, which follows the operation stage of said pipeline process, lower r bits Q_L of said operation result Q are recorded in said first memory, and upper bits Q_H of said operation result Q, excluding said bits Q_L, are recorded in said sixth register; and wherein, at a stage for reading variables to said registers, which follows said writing stage, simultaneously, a variable x_1 is read from said first memory and is stored in said first register, a variable x_3 is read from said second memory and is stored in said third register, and a variable x_5 is read from said third memory and is stored in said fifth register.

8. (original) The arithmetic circuit according to claim 7, wherein said first memory is a two-port memory having one data writing port and one data reading port, and said second memory and said third memories are single-port memories having one port for the writing and the reading of

data.

9. (original) An arithmetic method using an arithmetic circuit that includes an arithmetic unit, which has multiple input registers and multiple memories, comprising the steps of:

a1

performing an arithmetic operation based on values stored in said input registers;

writing the results of said arithmetic operation in said input registers or said memories; and

reading multiple variables from said multiple memories and storing said variables in said multiple input registers during the same pipeline stage.

10. (original) The arithmetic method according to claim 9, wherein said arithmetic unit is a multiplier adder for, based on values x_1, x_2, x_3 and x_4 having an r-bit length that are respectively input to a first register, a second register, a third register and a fourth register, providing the operation results Q for $x_1 + x_2 \cdot x_3 + x_4$ having a length of 2r bits or 2r+1 bits.

11. (original) The arithmetic method according to claim 10, wherein said multiple memories include a first memory and a second memory, further comprising:

a writing step in a pipeline process of said arithmetic unit for recording, in said first memory, lower r bits Q_L of said operation result Q, and for recording, in said fourth register, upper bits Q_H of said operation result Q, excluding said bits Q_L; and

a reading step of performing, at the sam reading stage in said pipeline process, the reading of a variable x_1 from said first

memory and storing said variable x_1 in said first register, and the reading of a variable x_3 from said second memory and storing said variable x_3 in said third register.

12. (original) The arithmetic method according to claim 11, wherein said first memory and said second memory are two-port memories having one data writing port and one data reading port.

a1

13. (original) The arithmetic method according to claim 11, wherein said first memory is a two-port memory having one data writing port and one data reading port, while said second memory is a single-port memory having one port for the writing and reading of data.

14. (original) The arithmetic method according to claim 9, wherein said arithmetic unit is a multiplier adder for, based on values x_1, x_2, x_3, x_4 x_5 and x_6, having an r-bit length, that are respectively input to a first register, a second register, a third register, a fourth register, a fifth register and a sixth register, and for providing the operation results Q for $x_1 + x_2 \cdot x_3 + x_4 \cdot x_5 + x_6$, which have a length of 2r bits or 2r+1 bits.

15. (original) The arithmetic method according to claim 14, wherein said multiple memories include a first memory, a second memory and a third memory, further comprising:

a writing step in a pipeline process of said arithmetic unit for recording, in said first memory, lower r bits Q_L of said operation result Q, and for recording, in said sixth register, upper bits Q_H of said operation result Q, excluding said bits Q_L; and

a reading step of performing, at the same reading stage of said pipeline process, the reading of a variabl x_1 from said first